

REMARKS

This Amendment is submitted in response to the Examiner's Action dated December 4, 2001, having a shortened statutory period set to expire March 4, 2002, extended to May 4, 2002.

In that Action the Examiner has objected to the drawings noting that the original drawings were objected to by the draftsman. Further, the Examiner believes that Figure 1 should be designated by a legend such as "Prior Art" because only that which is old is illustrated. Applicant respectfully disagrees and notes that Figure 1 is described in the present Specification as a data processing system which maintains multiple secure private keys in a non-secure storage in accordance with the method and system of the present invention. Thus, although Figure 1 appears to be an ordinary computer, when programmed in accordance with the teachings of the present invention that computer comprises the invention of the present application and thus Applicant urges that a legend such as "Prior Art" would be inappropriate.

Next, the Examiner objects to the drawings for failure to include the reference signs mentioned in the description at page 10, lines 26 and 28. Applicant urges the Examiner to consider that the reference signs specified by the Examiner are indeed present in the drawings and a parenthetical referral to the appropriate figure has been added by this amendment. Finally, the Examiner objects to the drawings because the reference character 204 in Figure 2 has been utilized to designate both the PCI bus bridge and the ISA bus bridge, noting page 8, lines 8 and 11. Applicant has corrected the Specification to conform to the drawings and the Examiner's objection to the drawings is therefore believed to be overcome. Applicant submits herewith formal drawings which reflect this situation.

Next, the Examiner rejects Claims 1-17 under 35 U.S.C. §102(e), as being anticipated by *Boneh, et al.*, U.S. Patent No. 6,134,660. That rejection, insofar as it might be applied to the

claims as amended herein, is respectfully traversed. *Boneh, et al.*, teach a system and method for revoking computer backup files utilizing cryptographic techniques. As illustrated in Figure 2 of *Boneh, et al.*, key file 204 is stored within system memory 104 and includes multiple encryption keys which are stored within protected memory so that only privileged processes may be allowed to read that memory and the content thereof. (See column 5, lines 63-67). Thereafter, *Boneh, et al.*, teaches that a master key is generated for each attempted backup and that master key is utilized within encryption engine 210 to store an encrypted copy of the key 208 within a backup or tape drive system. Thus, Applicant agrees with the Examiner that, at first blush, *Boneh, et al.*, may seem to disclose the storage of encryption keys within a non-secure memory by first encrypting those keys utilizing encryption engine 210.

However, on further examination the Applicant urges the Examiner to consider that the method and system of the present invention are directed to an asymmetrical key system. That is, a key system in which a public key is transmitted from one location to a second location and then utilized to encrypt a document which is then transmitted back to the owner of that public key where it can be decrypted only with the private key associated with that public key. Applicant urges the Examiner to consider that the key files stored within 204 and thereafter encrypted and stored in file 208 are not public or private keys but rather symmetrical keys which are utilized to both encrypt and decrypt a file.

Further, as amended by the present submission, Applicant's claims are now clearly directed to the maintenance of multiple secure private keys within non-secure storage. This is supported in the present Specification at numerous locations including page 3, lines 4-6. Thus, as the claims in the present Application now recite, multiple secure user private keys are stored in non-secure storage device utilizing a master key pair wherein the master public key is utilized to encrypt each of the multiple user's private keys wherein the master public key and private key are maintained in protective storage. Thus, each of the claims in the present Application, as amended

herein, expressly recites the encryption of multiple private keys utilizing a master public key in a manner not shown or suggested within *Boneh, et al.*

Indeed, *Boneh, et al.*, teaches the generation of a master key each time a backup is performed so that the master key is only utilized to encrypt a single symmetric key. Evidence of this interpretation is present throughout *Boneh, et al.* For example, at column 7, lines 24, *et seq.*, *Boneh, et al.* describes managing master keys by writing down the current master key and then, the operator "destroys his copy of the previous master key." Thus, it is clear that a particular master key is only utilized to encrypt a single symmetric key in the teaching of the *Boneh, et al.*, system.

In clear and direct contrast Claims 1-16, as amended herein, expressly recite the establishment of a master key pair which includes both a master private key and a master public key which are stored in protective storage. Thereafter, each of multiple private keys is encrypted utilizing the master public key and stored in non-secure storage so that any private key among multiple private keys may be retrieved and decrypted utilizing the master public key.

In this manner, as it is hoped the Examiner will appreciate, a particular user's private key may be accessed and decrypted only upon successful access to the master public key in a hierarchical approach to key protection.

As *Boneh, et al.*, is completely and absolutely deficient in any showing or suggestion of an asymmetrical key system in which both public keys and private keys are utilized to encrypt files, it is beyond cavil that *Boneh, et al.*, cannot be said to show or suggest the encryption of a private key utilizing a basis public key as expressly set forth within the present claims. Consequently, Applicant urges that the Examiner's rejection of Claims 1-16 under 35 U.S.C.

§103(e) as being anticipated by *Boneh, et al.*, is no longer valid and withdrawal of that rejection is respectfully requested.

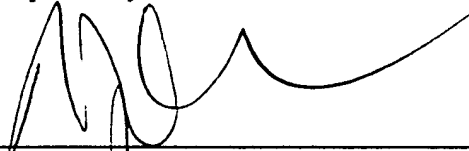
The Examiner has also rejected Claims 5-16 under 35 U.S.C. §103(a) as being unpatentable over *Boneh, et al.*, in view of *McBride*, U.S. Patent No. 6,292,899. That rejection is also respectfully traversed.

McBride is cited by the Examiner for its teaching of associating a user key pair with an application; however, nothing within *McBride* shows or suggests the novel encryption technique for encrypting the private key portion of an asymmetrical key system utilizing a basis public key in the manner set forth within the present claims. Consequently, Applicant urges that the Examiner's rejection of Claims 5-16 over this combination of references is no longer appropriate and withdrawal of that rejection is also respectfully requested.

A request for a two month extension of time and a check for the appropriate fee are enclosed herewith. No additional extension of time is believed to be required; however, in the

event an additional extension of time is required, please consider that extension requested and please charge the fee for that extension, as well as any other fee necessary to further the prosecution of this Application, to IBM Corporation Deposit Account No. **50-0563**.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'Andrew J. Dillon', written over a horizontal line.

Andrew J. Dillon

Reg. No. 29,634

BRACEWELL & PATTERSON, L.L.P.

Suite 350, Lakewood on the Park

7600B North Capital of Texas Highway

Austin, Texas 78731

(512) 542-2100

ATTORNEY FOR APPLICANTS

IN THE SPECIFICATION:

Please amend the Specification as follows:

Please substitute the paragraph beginning at page 8, line 11 and ending at page 8, line 11 with the following:

--CPU 200 is connected by address, control, and data busses 202 to a memory controller and peripheral component interconnect (PCI) bus bridge 204 which is coupled to system memory 206. An integrated drive electronics (IDE) device controller 220, and a PCI bus to Industry Standard Architecture (ISA) bus bridge [204] 212 are connected to PCI bus bridge 204 utilizing PCI bus 208. IDE controller 220 provides for the attachment of IDE compatible storage devices, such a removable hard disk drive 222. PCI/ISA bridge 212 provides an interface between PCI bus 208 and an optional feature or expansion bus such as the ISA bus 214. PCI/ISA bridge 212 includes power management logic. PCI/ISA bridge 212 is supplied power from battery 244 to prevent loss of configuration data stored in CMOS 213.--

Please substitute the paragraph beginning at page 10, line 26 and ending at page 10, line 26 with the following:

--**Figure 3** illustrates a high level flow chart which depicts establishing and storing a master key pair in protected storage in a data processing system in accordance with the method and system of the present invention. The process starts as depicted at block 300 and thereafter passes to block 302 which illustrates establishing a master key pair for data processing system 30 (see **Figure 1**). Next, block 304 depicts the storage of the master public key and master private key in protected storage 262 (see **Figure 2**) which is a one-time writable, protected storage. The process then terminates as illustrated at block 306.--

REDACTED CLAIMS

1 --1. (Amended) A method in a data processing system for maintaining multiple secure user
2 private keys in a non-secure storage device, said method comprising the steps of:

3 establishing a master key pair for said system, said master key pair including a master
4 private key and a master public key;

5 storing said master key pair in a protected storage device;

6 establishing a unique user key pair for [a] each of multiple users, each of said user key
7 pairs including a user private key and a user public key;

8 encrypting each of said user private keys utilizing said master public key; and

9 storing each of said encrypted user private keys in said non-secure storage device,
10 wherein each of said encrypted user private keys is secure while stored in said non-secure storage
11 device.--

1 2. (Unchanged) The method according to claim 1, further comprising the steps of:

2 establishing an encryption device having an encryption engine and said protected storage
3 device; and

4 said protected storage device being accessible only through said encryption engine.

1 --3. (Amended) The method according to claim 2, further comprising the step of said encryption
2 engine encrypting each of said user private keys utilizing said master public key stored in said
3 protected storage device.--

1 --4. (Amended) The method according to claim 3, further comprising the steps of:

2 an application generating a message to transmit to a recipient;

3 said encryption engine decrypting [said] a particular user's private key utilizing said
4 master private key;

5 said encryption engine encrypting said message utilizing said decrypted particular user's
6 private key and [a] said recipient's public key; and

7 said system transmitting said encrypted message to said recipient.--

1 --5. (Amended) The method according to claim 4, wherein the step of establishing a unique user
2 key pair for each of multiple users further comprises the step of associating each said user key
3 pair with an application.--

1 --6. (Amended) The method according to claim 5, further comprising the steps of:

2 establishing a certificate, said certificate being associated with said application, said
3 particular user's private key, and said particular user;

4 in response to said particular user attempting to access said application utilizing said
5 certificate, said encryption engine utilizing said certificate to determine a location within said
6 non-secure storage device for said particular user's private key associated with said certificate;

7 said encryption engine decrypting said particular user's private key; and

8 said encryption engine utilizing said decrypted particular user's private key to encrypt
9 messages transmitted by said application.--

1 --7. (Amended) The method according to claim [6] 1, wherein said step of storing each of said
2 encrypted user private keys in said non-secure storage further comprises the step of storing each
3 of said encrypted user private keys in a hard drive.--

1 --8. (Amended) The method according to claim 7, further comprising the step of each of said
2 unique user key pairs being capable of being utilized only in said data processing system wherein
3 [said] a particular user key pair is established, wherein said particular user key pair is not capable
4 of being utilized in a second data processing system.--

1 --9. (Amended) A data processing system for maintaining multiple secure user private keys in a
2 non-secure storage device, comprising:

3 an encryption device included within said system for establishing a master key pair for
4 said system, said master key pair including a master private key and a master public key;

5 a protected storage device for storing said master key pair;

6 said encryption device executing code for establishing a unique user key pair for [a] each
7 of multiple users, each of said user key pairs including a user private key and a user public key;

8 said encryption device executing code for encrypting each of said user private keys
9 utilizing said master public key; and

10 [said] a non-secure storage device for storing each of said encrypted user private keys,
11 wherein each of said encrypted user private keys is secure while stored in said non-secure storage
12 device.--

1 10. (Unchanged) The system according to claim 9, further comprising:

2 said encryption device including an encryption engine and said protected storage device;
3 and

4 said protected storage device capable of being accessed only through said encryption
5 engine.

1 --11. (Amended) The system according to claim 10, further comprising said encryption engine
2 executing code for encrypting each of said user private keys utilizing said master public key
3 stored in said protected storage device.--

1 --12. (Amended) The system according to claim 11, further comprising:

2 an application capable of generating a message to transmit to a recipient;

3 said encryption engine executing code for decrypting [said] a particular user's private key
4 utilizing said master private key;

5 said encryption engine executing code for encrypting said message utilizing said
6 decrypted particular user's private key and [a] said recipient's public key; and

7 said system transmitting said encrypted message to said recipient.--

1 --13. (Amended) The system according to claim 12, further comprising said system executing
2 code for associating each said user key pair with an application.--

1 --14. (Amended) The system according to claim 13, further comprising:

2 said system executing code for establishing a certificate, said certificate being associated
3 with said application, said particular user's private key, and said particular user;

4 in response to said particular user attempting to access said application utilizing said
5 certificate, said encryption engine executing code utilizing said certificate for determining a
6 location within said non-secure storage device for said particular user's private key associated
7 with said certificate;

8 said encryption engine executing code for decrypting said particular user's private key
9 pair; and

10 said encryption engine capable of utilizing said decrypted particular user's private key to
11 encrypt messages transmitted by said application.--

1 --15. (Amended) The system according to claim 14, further comprising said system executing
2 code for storing each of said encrypted user private keys in a hard drive.--

1 --16. (Amended) The system according to claim 15, further comprising each of said unique user
2 key pairs being capable of being utilized only in said data processing system wherein [said] a
3 particular user key pair is established, wherein said particular user key pair is not capable of
4 being utilized in a second data processing system.--

Please cancel Claim 17.

1/3

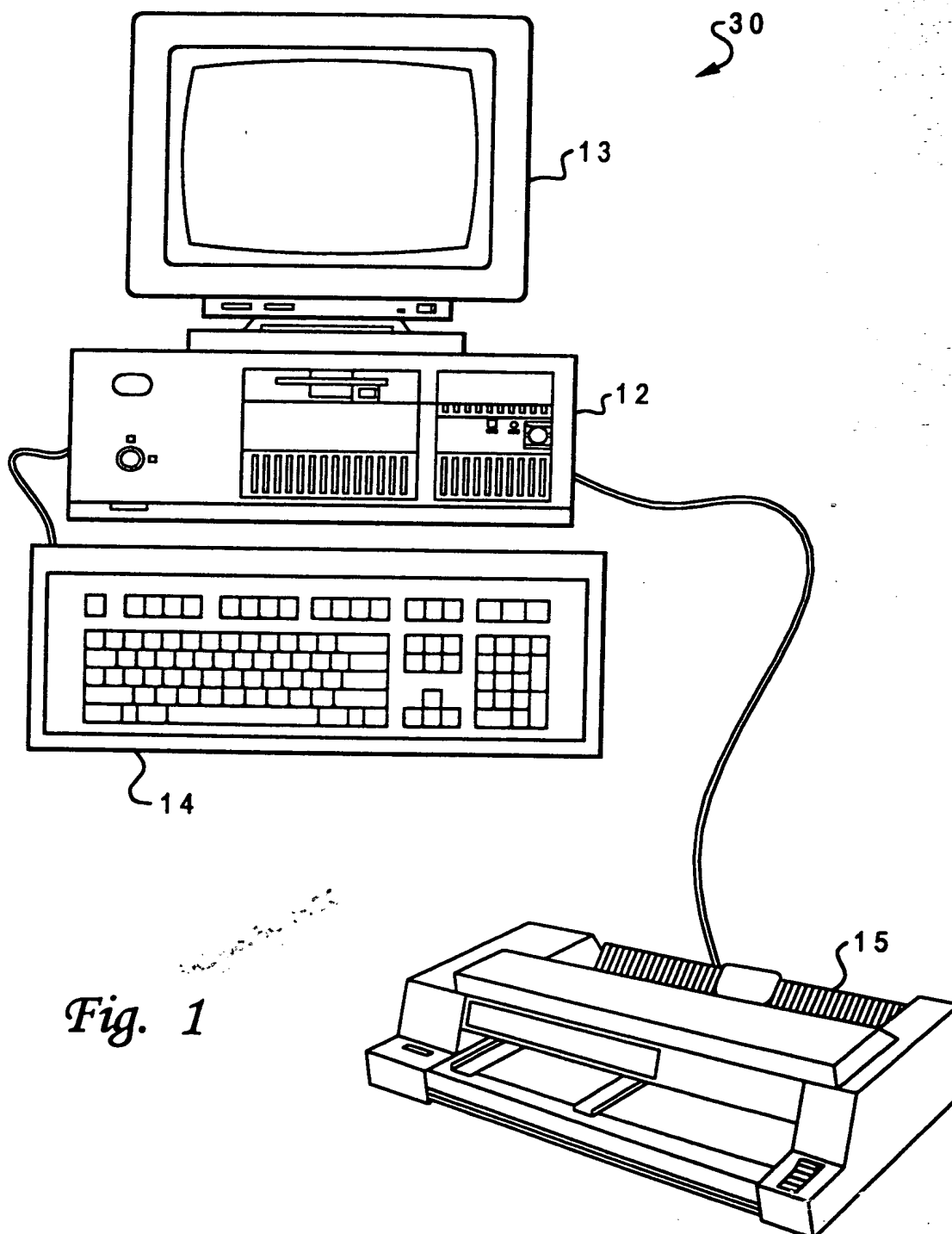


Fig. 1

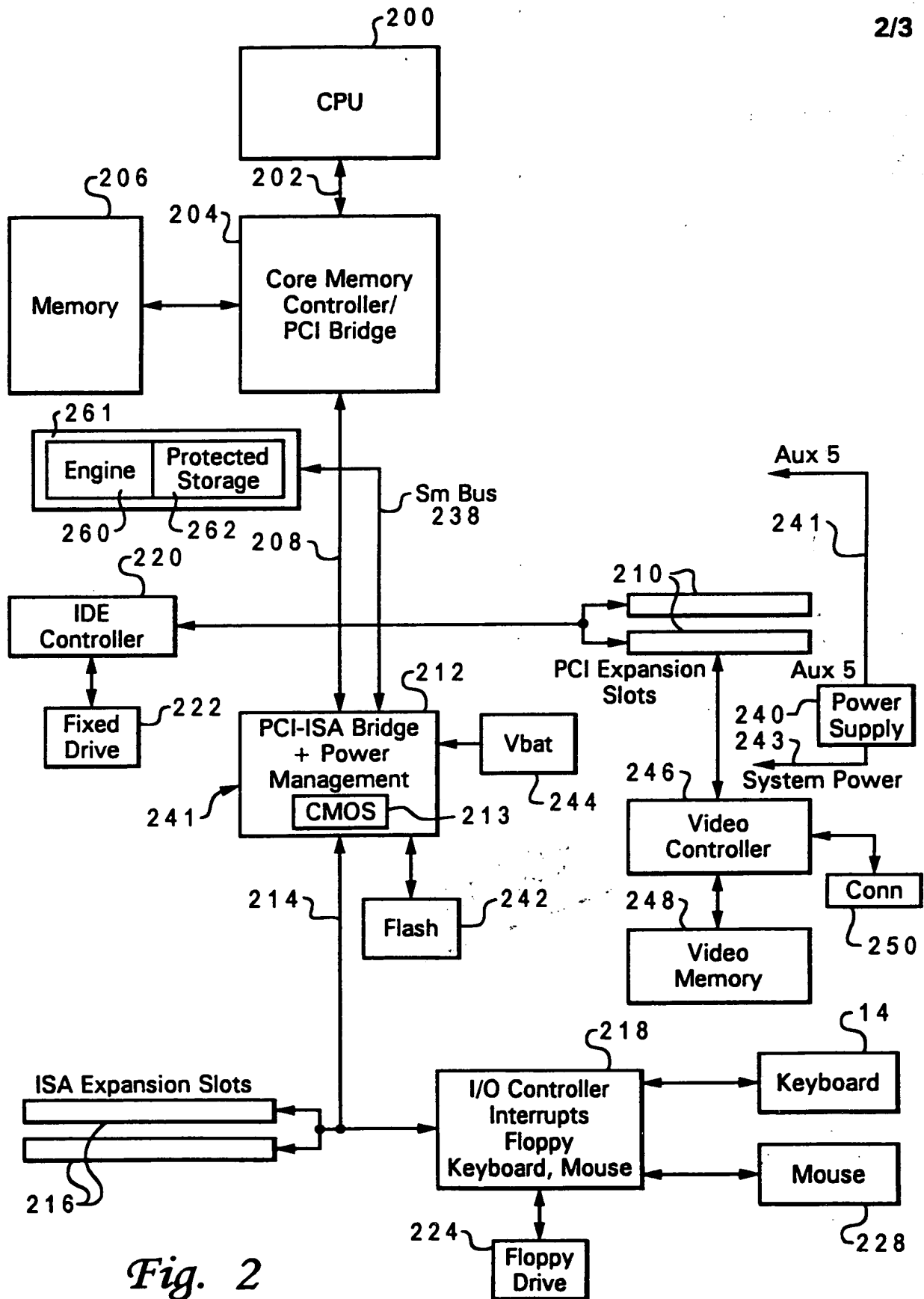


Fig. 2

3/3

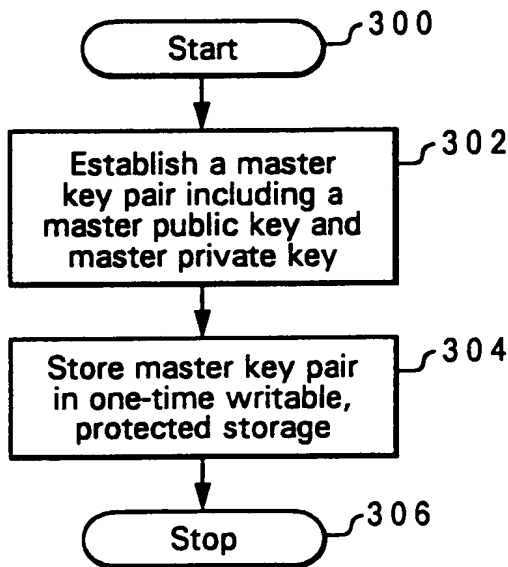


Fig. 3

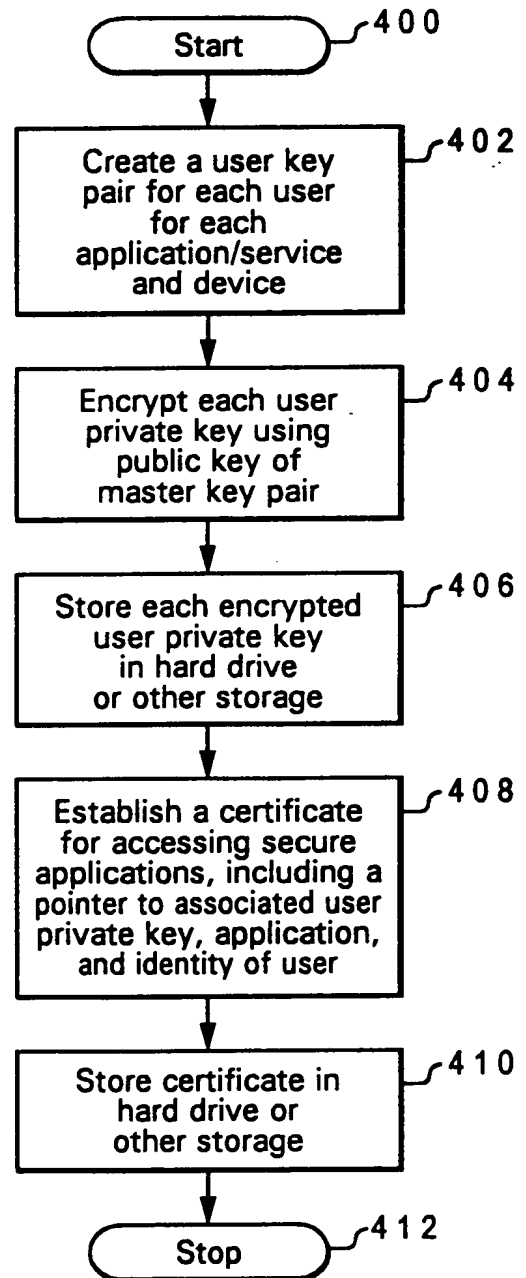


Fig. 4

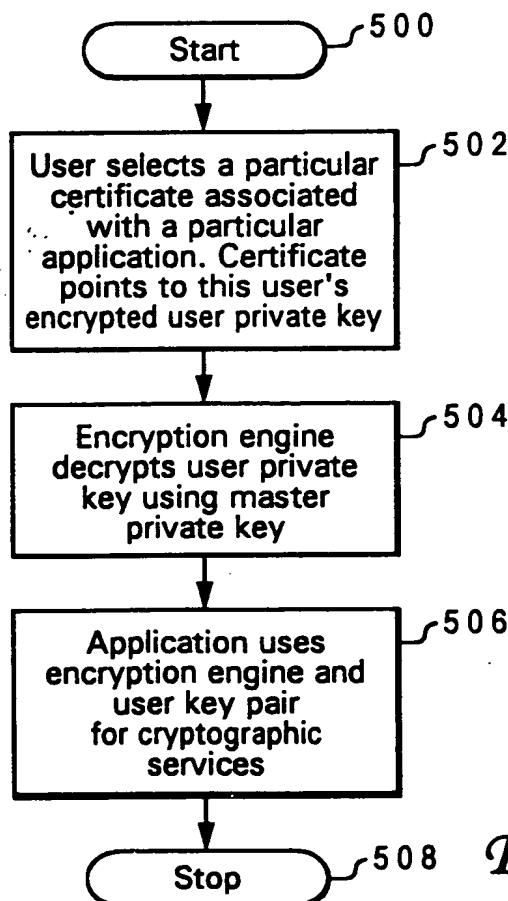


Fig. 5